#17 Brief
PD
PATENT 10/22/03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of John Philip PETTITT	:	Confirmation No.: 5428
	:	Group Art Unit: 3625
Serial No.: 09/442,106	:	
	:	Examiner: Yogesh C. Garg
Filed: November 17, 1999	:	

For: METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER A COMPUTER NETWORK

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Further to the Notice of Appeal filed August 7, 2003, the Applicant hereby submits its appeal brief.

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on: October 10, 2003 by: Teresa Austin

REAL PARTY IN INTEREST

The real party in interest is CyberSource Corporation, Mountain View, California.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-16 of the original application have been canceled. Claims 17-30 were added by previous amendment and are pending.

Applicant is appealing the final rejection of Claims 17-30.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to final rejection.

SUMMARY OF INVENTION

A percentage of all purchase transactions conducted by a consumer and a merchant over the Internet are known to involve fraud. For example, stolen credit cards are sometimes used to order products by individuals who provide a shipping address different from the billing address associated with the credit card. The merchant ships product to the shipping address, the true owner of the card disputes the resulting credit card charge amount, and the merchant cannot collect the price of the product. The invention provides a method and system for detecting fraud in a credit card transaction performed over a computer network. In one embodiment, the invention is performed in computer software by a service provider that receives information from a merchant for a proposed transaction, and returns a score value indicating the fraud risk associated with the transaction. Unlike prior systems or methods, the invention integrates multiple checks and cross-checks, including a cross-check of an Internet address of the prospective purchaser against physical addresses previously associated with that purchaser, to arrive at a fraud score that more accurately predicts whether the transaction will be fraudulent.

Claim 17 is representative. A transaction involves the consumer purchasing a product from the merchant using a credit card. The method comprises receiving, from the merchant, transaction information that identifies the consumer and the product, including an Internet address of the consumer. Credit card information associated with the consumer that identifies the credit card to be used in the transaction is also received.

The credit card information is verified based upon a consistency check that determines whether the credit card information matches the consumer (FIG. 3, block 204; specification, p. 4, p. 5). The credit card information is also verified based upon a history check that determines whether the credit card information is consistent with the transaction information (FIG. 3, block 202; p. 4). The credit card information is further verified based upon an automatic verification system (AVS) (FIG. 3, block 206). Standalone AVS systems have been used in the prior art apart from the method as claimed, but are insufficient alone to enable a merchant to fully evaluate transaction risk.

The credit card information is further verified using an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer (pp. 6-7). For example, if a prospective purchaser with an Internet address of "joe@domain.com" specifies a shipping address in Alabama, but all prior transactions associated with that purchaser had a shipping address in California, then the proposed transaction is likely to be fraudulent. Moreover, the proposed transaction is more likely to be fraudulent than if the purchaser provided a different shipping address in California than shown in the database.

Based on all the verification steps taken together, the method creates and stores a fraud score value based steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

GROUPING OF CLAIMS

The claims stand or fall together.

ISSUES

1. Whether the Office Action properly rejected Claims 17-30 under non-statutory obviousness-type double patenting;
2. Whether the Office Action properly rejected Claims 17-26 and 28-30 as unpatentable under 35 U.S.C. §103(a) over Wallace U.S. Pat. No. 5,988,497 in view of McCrea et al. and further in view of Gopinathan et al. U.S. Pat. No. 5,819,226; and
3. Whether the Office Action properly rejected Claim 27 under 35 U.S.C. §103(a) over Wallace/McCrea/Gopinathan and further in view of Richardson.

ARGUMENT

I. **The Office Action Erred in Failing to Enter the Terminal Disclaimer**

The Office Action mailed October 28, 2002 rejected Claims 17-30 based on the non-statutory, judicially created doctrine of obviousness-type double patenting. In a reply filed February 28, 2003, the Applicant presented a proper Terminal Disclaimer signed by an attorney of record in the application. The Office Action refused to enter the Terminal

Disclaimer, contending that "the person who signed the terminal disclaimer is not recognized as an officer of the assignee, and he/she has not been established as being authorized to act on behalf of the assignee. See MPEP §324."

The Office Action is erroneous. An attorney or agent of record in an application may execute a terminal disclaimer, as provided in 37 C.F.R. §1.321(b)(1)(iv). The same section applies to terminal disclaimers filed to obviate a rejection based on the judicially created doctrine of obviousness-type double patenting, 37 C.F.R. §1.321(c). Indeed, the USPTO's own terminal disclaimer form, Form PTOISB/26, approved for use October 31, 2002, includes a checkbox with which the signing individual may assert that he or she is an attorney or agent of record without separately establishing authority to act. See Exhibit 1, attached hereto.

MPEP 324 is not germane. In the present case, the attorney who signed the Terminal Disclaimer holds a valid power of attorney from the assignee. An attorney signing a Terminal Disclaimer need not establish authority to act on behalf of the assignee; however, even if such a requirement existed, the attorney's signature on the Terminal Disclaimer is a representation that the attorney is empowered to act for the assignee.

Therefore, the previously filed Terminal Disclaimer fully complies with applicable rules and law, and the Office Action's refusal should be reversed. If the Terminal Disclaimer is entered, then the rejection of Claims 17-30 based on double patenting is traversed.

II. The Office Action Erred in Rejecting Claims 17-26 and 28-30 Under 35 U.S.C. §103(a) over Wallace in view of McCrea et al. and Gopinathan et al.

The Office Action rejected Claims 17-26 and 28-30 as allegedly unpatentable under 35 U.S.C. §103(a) over Wallace ("Wallace"; U.S. Patent No. 5,988,497) in view of McCrea et al. ("McCrea"; "The Internal Report") and further in view of Gopinathan et al. ("Gopinathan"; U.S. Patent No. 5,819,226). The rejection is erroneous and should be reversed.

With respect to Claim 17, there is no suggestion or motivation to one skilled in the art to combine the teachings of Wallace and McCrea and Gopinathan to arrive at the invention recited in Claim 17. Thus, a prima facie case of obviousness has not been established based on the references of record.

The Office Action is correct that "Wallace fails to teach use of an Internet address in the detection of fraud in a credit card transaction by verifying if the information about physical addresses associated with the internet addresses used in the transactions are consistent." However, the Office Action erroneously alleges that "[i]n view of McCrea it would have been obvious ... to modify Wallace to use Internet address in detecting credit card fraud detection by verifying information about physical address associated with the Internet address used in the transaction." McCrea does not teach the subject matter of the claim, and there is no suggestion to apply the teachings of McCrea in the field of fraud control.

McCrea is a report prepared for the Australian Taxation Office. At most, McCrea describes use of an IP address to determine whether an associated host is within Australia based on connections of Australia to the Internet and on subnet address ranges that collectively define all IP addresses in Australia. Thus, at most, McCrea teaches how to determine the **absolute** location of a computer. McCrea only addresses the question, **is a given computer's IP address within Australia?** But McCrea does not disclose comparing

consistency of one **physical** address with another, as claimed, which is an entirely different issue.

For example, McCrea does not suggest determining whether an IP address that is found to be in Australia is consistent with other known geographic locations of the same known user or computer. In contrast, Claim 17 recites determining "whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer." The claim does not recite determining the absolute location of a consumer, but whether the current address provided by the consumer is consistent with other addresses previously provided for other transactions. **McCrea is silent on consistency of past addresses.** For this reason alone, McCrea in combination with Wallace fails to teach the subject matter of Claim 17.

McCrea provides no teaching or suggestion of linking an Internet address with a physical address, beyond the level of determining whether the Internet address is associated with subnets in Australia. Further, McCrea does not access a **database of historical transaction records** for **verification** purposes with respect to the link between a given Internet address and associated physical address(es).

The apparent purpose of the described process is for determining whether online purchases by the host could be **subject to Australian sales tax**. There is no suggestion to apply McCrea in the field of **fraud detection**, to which Claim 17 is directed. McCrea is not "in the field of the applicant's endeavor," see In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992).

The Office Action states that McCrea "...is analogous to the limitation recited in claim 1 ..." (Office Action, page 3, section 3.2(i)). Addressing an analogous issue does not suggest the same subject matter as the claim. Relying on analogy is legally insufficient to support a §103 rejection.

The Action attempts to stitch together features from **three different references** using the claim as an instruction manual to find prior art that allegedly renders Claim 17 obvious, thereby impermissibly applying hindsight. The Court of Appeals for the Federal Circuit (CAFC) has stated that:

> [I]t is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. This court has previously stated that "[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention."

In re Fritch, 972 F.2d 1260, 23 USPQ 2d 1780, 1784 (Fed. Cir. 1992). While the techniques taught in the present application have become commonplace in Internet commerce, the application is entitled to an effective filing date, based on priority, of at least as early as July 28, 1997. The parent application was filed **more than six years ago**. The Office must be especially diligent to avoid impermissible reliance on hindsight.

The Office Action replies to Applicant's assertion of hindsight by relying on In re McLaughlin, 443 F.2d, 1392, 170 USPQ 209 (CCPA 1971). However, the logic of McLaughlin is internally contradictory, and for that reason has not been followed in contemporary cases. McLaughlin suggests that hindsight reconstruction of the claimed invention is proper "so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure." Office Action at p. 4. But the selection and interpretation of the references in an Office Action **is inevitably and necessarily influenced by applicant's disclosure**. For example, the contention that determining the absolute location of a computer in Australia is "analogous" to determining consistency of previously used physical addresses **is necessarily informed by applicant's disclosure**. McLaughlin is not followed in contemporary case law because its decisional framework is fundamentally flawed.

In this case, it would not have been obvious to one skilled in the relevant art at the time of the invention to combine the cited references at least for the reason that one would not look to McCrea for teachings with respect to fraud detection and control. Further, one skilled in the art would not look to McCrea, which is in the field of taxation, for a teaching regarding "**verifying** the credit card information based upon an Internet identification system that determines whether a **physical address** specified in the transaction information is **consistent with other physical addresses** that have been **specified in a database of records of other transaction information for other transactions** that are associated with the Internet address of the consumer," as recited in Claim 17.

The McCrea disclosure (1) fails to teach the feature of Claim 17 on which the Office Action relies; (2) fails to suggest a combination with the non-analogous teachings of Wallace and Gopinathan; and (3) is in a field that is not analogous with fraud detection. In general, the Office Action refuses to recognize and acknowledge the non-obviousness of **integrating an Internet address-based feature into a Internet credit card fraud detection process, utilizing a database of historical transaction information, through verification of a current physical address in view of historical physical addresses associated with the same Internet address**. The complex process recited in Claim 17 should not stand rejected as obvious at the time of invention based on a convoluted combination of disparate references.

Furthermore, the CAFC has stated that "the actual determination of the [obviousness] issue requires an *evaluation ... of the claimed invention as a whole*" (emphasis added; Lear Siegler, Inc. v. Aeroquip Corp., 733 F.2d 881, 221 USPQ 1025, 1033 (Fed. Cir. 1984)). Hence, each feature of a claim should be evaluated in view of the subject matter of the entire claim and in view of the feature's interaction with other features in the claim.

In this case, reliance on three references for an obviousness rejection, one of which is not in the same field as the other references, gives the appearance of piecemeal evaluation of the invention. For all of the foregoing reasons, a prima facie case of obviousness has not been made. Therefore, Claim 17 is patentable over the references of record and reversal of the rejection of Claim 17 is respectfully requested.

Claims 18-23 depend directly or indirectly from Claim 17, and are thus patentable over the prior art of record for at least the same reasons presented above in reference to Claim 17. Therefore, reversal of the rejection of Claim 18-23 is respectfully requested.

Claim 21 in conjunction with its parent Claim 17 recite weighting each verification step according to importance **determined by the merchant**. At paragraph 5, the Office Action takes official notice "of both the concept and benefits to accord weights to various parameters, and weights being determined based upon the importance assigned to each parameter as per ones own discretion, to arrive at a final score/total to evaluate a performance. For example, it is well known that teachers assign different weights to quizzes, home assignments, class-work and tests while evaluating the performance and to award a final and cumulative grade to the student." However, official notice is allowed only for facts that are capable of such instant and unquestionable demonstration as to defy dispute. In re Ahlert, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970) (citing In re Knapp Monarch Co., 296 F.2d 230, 132 USPQ 6 (CCPA 1961)). Providing a weighting capability to a merchant, **as a client of a fraud detection service or method**, is not capable of instant and unquestionable determination.

In section 3.2(iv) of the Office Action, page 6, the Office Action asserts that "the Official Notice ... was directed to the old and well-known concept that teachers assign different weights-also corresponds to the importance-to quizzes, home assignments, class-work, and tests while evaluating the performance and to award a final and cumulative grade to the student renders the claimed limitation of claim 21 obvious." Applicants disagree. The Office Action apparently proposes that teachers invariably assign the same number of points to assignments—i.e., all tests are worth 100 points—and then apply weighting factors to make some more important and others less important. But this is not what teachers do. Common practice in the classroom is to assign different total point values to different assignments—a 100-point test, a 10-point quiz, etc., so that the total number of points at the end of a grading period accurately reflects the importance of each individual assignment.

Thus, the subject matter of the Official Notice is not capable of "instant and unquestionable determination, as required for Official Notice. Moreover, reliance on anecdotal evidence of classroom practice, for a rejection of a claim relating to data processing in the field of merchant transaction processing, is preposterous and is exactly the kind of non-analogous art approach that the courts have consistently rejected. Because the Official Notice with respect to letting merchants determine weights is an insufficient basis for the rejection of Claim 21, the rejection should be reversed.

Claim 24 is an independent claim that includes steps of (1) verifying credit card information based on an Internet identification system that determines consistency between a physical address and an Internet address associated with a consumer in a transaction; and (2) receiving from a merchant weight values associated with each of a plurality of mechanisms for detecting fraud in a credit card transaction. Each of these features has been discussed above in reference to Claim 17 and Claim 21, respectively. Thus, based on the foregoing reasons, the references of record do not teach, disclose, or suggest these features. Therefore, a prima facie case of obviousness is not established and Claim 24 is patentable over the references of record. Reversal of the rejection of Claim 24 is respectfully requested.

Claims 25-27 depend directly or indirectly from Claim 24, and are thus patentable over the prior art of record for at least the same reasons presented above in reference to Claim 24. Therefore, reversal of the rejection of Claim 25-27 is respectfully requested.

III. The Office Action Erred in Rejecting Claims 17-26 and 28-30 Under §103(a) over Wallace, McCrea et al., Gopinathan et al. and Richardson

Paragraph 6 of the Office Action rejected Claim 27 under 35 U.S.C. §103(a) as allegedly unpatentable over Wallace in view of McCrea, further in view of Gopinathan, further in view of Richardson. Applicant respectfully traverses this rejection.

With respect to Claim 27, the Office Action contends that Richardson teaches the construction and use of maps of credit card transactions. However, Richardson does not teach, disclose or suggest constructing a map of credit card transactions that **utilize a specific Internet address** that is identified with the transaction. Furthermore, as discussed above in reference to Claim 17, none of the references of record teach, suggest or make obvious the use of Internet addresses in the manner used in the present application. Therefore, Claim 27 would not have been obvious in view of the references of record, and the rejection of Claim 27 should be reversed.

At page 6, section 3.2(v), the Office Action responds by asserting that an applicant cannot overcome a §103 rejection based on a combination of references by attacking a single reference. This is an immaterial procedural point that has not prevented courts from reversing multi-reference §103 rejections when the proposed combination does not reach the complete subject matter of the claim. Indeed, the statutory language of §103 unequivocally provides that obviousness may be found only when the prior art shows "the subject matter sought to be patented ... **as a whole**." 35 U.S.C. §103(a) (emphasis added). If, as here, a proposed combination does not disclose, teach or suggest all features of the claimed invention because one feature is missing from one of the references relied upon, then §103 cannot form the basis of a rejection.

In addition, the Office Action does not reply in substance to Applicant's technical argument concerning Claim 27.

Claim 28 is a system claim and Claim 29 is a computer-readable medium claim, both of which comprise features similar to method Claim 17. Therefore, Claims 28 and 29 are patentable over the references of record for at least the same reasons given above for Claim 17. Reversal of the rejections of Claims 28 and 29 is respectfully requested.

Claim 30 is an independent claim that includes use of an Internet verification system to verify credit card information by determining whether a physical address specified in transaction information is consistent with other physical addresses specified in a database of transaction information for other transactions associated with the consumer's Internet address. As shown above in reference to Claim 17, the references of record do not teach, disclose, suggest or make obvious the use of an Internet verification system that functions with respect to physical and Internet addresses, as described and claimed in the application. Hence, Claim 30 is also patentable over the references of record for at least the same reasons as Claim 17 and, therefore, reversal of the rejection of Claim 30 is respectfully requested.

IV. Conclusion

For the reasons indicated above, all pending Claims 17-30 present subject matter that is patentable over the references of record, and are in condition for allowance. Therefore, Applicants respectfully request reversal of the final rejections expressed in the Office Action.

A petition for extension of time under 37 C.F.R. §1.136 to the extent necessary to make this paper timely filed is hereby made.

Throughout the pendency of this application the Commissioner is hereby authorized to charge any applicable fee, including extension of time fees, and to credit any overpayment to our Deposit Account No. 50-1302.

Respectfully Submitted,

JOHN P. PETTIT
CYBERSOURCE CORPORATION

Date: October 10, 2003

By Christopher
Christopher J. Palermo
Reg. No. 42,054

Hickman Palermo Truong & Becker LLP
1600 Willow Street
San Jose, CA 95125-5106
Tel. (408) 414-1080 x202
Fax (408) 414-1076

APPENDIX

17. A method for detecting fraud in a transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the method comprising the steps of:

receiving, from the merchant, transaction information that identifies the consumer and the product, including an Internet address of the consumer;

receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;

verifying the credit card information based upon a history check that determines whether the credit card information is consistent with the transaction information;

verifying the credit card information based upon an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

18. A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

receiving, from the merchant, transaction information that identifies the consumer and the product, including an Internet address of the consumer and a shipping address for the product;

retrieving, from the database of the Internet identification system, a plurality of records of other transaction information that are associated with the Internet address of the consumer;

determining whether a physical address contained in each of the plurality of records matches the shipping address in the transaction information;

verifying the credit card information when the physical address matches the shipping address in the transaction information.

19. A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in other transaction information for other transactions associated with an Internet email address of the consumer.

20. A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

retrieving a plurality of records of other transactions from an Internet identification system that associates the credit card number with other physical addresses that have been specified in other transaction information for other transactions associated with an Internet address of the consumer;

creating and storing a map of the other transactions;

verifying the credit card information based upon the map of other transactions, by determining whether a physical address specified in the transaction information is consistent with the other physical addresses in the other transaction information.

21. A method as recited in claim 17, further comprising the step of:

weighting each of the verifying steps according to an importance as determined by the merchant of each verifying step to the credit card transaction.

22. A method as recited in claim 17, wherein the step of verifying the credit card information based upon a history check comprises the step of:

receiving, from other merchants, records of other transactions involving the other merchants and the consumer;

storing the records of other transactions in a transaction history database that can be accessed and supplemented by other merchants with information about other credit card transactions with the consumer and such other merchants;

verifying the credit card information based upon the transaction history database by determining whether the credit card information is consistent with the records of other transactions in the transaction history database.

23. A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

receiving, from other merchants, records of other transactions involving the other merchants and the consumer;

storing the records of other transactions in an Internet identification database that can be accessed and supplemented by other merchants with information about other credit card transactions with the consumer and such other merchants;

verifying the credit card information based upon the Internet identification database by determining whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in records of the Internet identification database for other transactions associated with an Internet address of the consumer.

24. A method for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet comprising the steps of:

receiving, from the consumer, credit card information relating to the transaction;

creating and storing a consistency check mechanism, a transaction history check mechanism, an automatic verification mechanism and an Internet identification mechanism, each of which may indicate whether the credit card transaction is fraudulent based on transaction information, in combination with information that identifies the consumer, in which the transaction information provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent;

receiving from the merchant and storing a weight value associated with each of the mechanisms and storing the weight value in association with information that identifies the mechanisms, wherein each of the weight values signifies an importance to the merchant of the value to the credit card transaction of the associated mechanism;

weighting each value of the plurality of parameters according to weight values;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

25. A method as recited in claim 24 wherein the steps of creating and storing further include:

creating and storing a transaction history check mechanism that includes a transaction history database which can be accessed and supplemented by other merchants with information about transactions of the consumer with such other merchants.

26. A method as recited in claim 24 wherein the steps of creating and storing further include:

creating and storing an Internet identification verification system (IIS) mechanism that includes an Internet address database that can be accessed and supplemented with new Internet addresses as Internet address expansion occurs.

27. A method as recited in claim 24 wherein the steps of creating and storing further include:

obtaining other transactions utilizing an Internet address that is identified with the credit card transaction;

constructing a map of credit card transactions based upon the other transactions;

utilizing the map of credit card transactions to determine if the credit card transaction is valid.

28. An integrated verification system for determining whether a transaction between a merchant and consumer over the Internet is fraudulent, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the system comprising:

means for receiving, from the merchant, transaction information that identifies the consumer and the product;

means for receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

means for verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;

means for verifying the credit card information based upon a transaction history check that determines whether the credit information is consistent with the transaction information;

means for verifying the credit card information based upon an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other that are associated with the Internet address of the consumer;

means for creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

29. A computer readable medium containing program instructions for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, wherein execution of the program instructions by one or more processors of a computer system causes the one or more processors to carry out the steps of:

receiving, from the merchant, transaction information that identifies the consumer and the product;

receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in 1the transaction;

verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;

verifying the credit card information based upon a transaction history check that determines whether the credit card information is consistent with the transaction information;

verifying the credit card information based upon an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

30. A method for detecting fraud in a transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the method comprising the steps of:

receiving, from the merchant, transaction information that identifies the consumer and the product;

receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer, a transaction history check that determines whether the credit card information is consistent with the transaction information, and an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

PTOISB/26 (10-00)
Approved for use 10/31/2002. OMB 0651-0031
U.S. Patent end Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A PRIOR PATENT	Docket Number (Optional)

In re Application of:

Application No.:

Filed:

For:

The owner*, ________, of _______ percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application, which would extend beyond the expiration date of the full statutory term defined in 35 U S C 154 to 156 and 173, as presently shortened by any terminal disclaimer, of prior Patent No. ________. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 to 156 and 173 of the prior patent, as presently shortened by any terminal disclaimer, in the event that it later: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of an organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. □ The undersigned is an attorney or agent of record.

________________________ Signature   ____________ Date

________________________ Typed or printed name

□ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement Under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Box Patent Application, Washington, DC 20231.